State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory

March 08, 2016

The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

ADVISORY NUMBER:
SA2016-037

DATE(S) ISSUED:
03/08/2016

SUBJECT:
Multiple Vulnerabilities in Google Android OS Could Allow for Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Google Android operating system (OS), the most severe of which could allow for remote code execution. Android is an operating system developed by Google for mobile devices including, but not limited to smartphones, tablets, and watches. These vulnerabilities could be exploited through multiple methods including email, web browsing and MMS when processing media files. Successful exploitation of these vulnerabilities could result in remote code execution in the context of the application, an attacker gaining elevated privileges, blocking access to a Bluetooth device, or bypassing security restrictions.

THREAT INTELLIGENCE:
There are no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
Android OS builds prior to LMY49H and versions prior to 6.0 without Security Patch Level of March 1st, 2016

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**

- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:

Google's Android OS is prone to multiple vulnerabilities, the most severe of which could allow for remote code execution. The vulnerabilities are as follows:

- Multiple remote code execution vulnerabilities in the 'Mediaserver' service when it processes a specially crafted media file. (CVE-2016-0815, CVE-2016-0816)
- A remote code execution vulnerability in the 'libvpx' service when it processes a specially crafted media file. (CVE-2016-1621)
- An elevation of privilege vulnerability in 'Conscrypt' that could allow for a local malicious application to execute arbitrary code within the kernel. (CVE-2016-0818)
- An elevation of privilege vulnerability in the 'Kernel Keyring Component' component that could allow for a local malicious application to execute arbitrary code within the device root context. (CVE-2016-0728)
- A mitigation bypass vulnerability in the kernel that could allow for a local malicious application to execute arbitrary code within the kernel. (CVE-2016-0821)
- An information disclosure vulnerability in the kernel that could allow for a bypass of security measures in place to increase the difficulty of attackers exploiting the platform. (CVE-2016-0823)
- An information disclosure vulnerability in 'libstagefright' that could allow for a bypass of security measures in place to increase the difficulty of attackers exploiting the platform. (CVE-2016-0824)
- Multiple elevation of privilege vulnerabilities in 'Mediaserver' that could allow for a local malicious application to execute arbitrary code within the kernel. (CVE-2016-0826, CVE-2016-0827)
- Multiple information disclosure vulnerabilities in 'Mediaserver' that could allow for a bypass of security measures in place to increase the difficulty of attackers exploiting the platform. (CVE-2016-0828, CVE-2016-0829)
- A remote denial of service vulnerability in the 'Bluetooth' component could allow a proximal attacker to block access to an affected device. (CVE-2016-0830)
- An information disclosure vulnerability in the 'Telephony' component that could allow an application to access sensitive information. (CVE-2016-0831)
- An elevation of privilege vulnerability in the 'Setup Wizard' could enable an attacker who had physical access to the device to gain access to device settings and perform a manual device reset. (CVE-2016-0832)

Successful exploitation of these vulnerabilities could result in remote code execution in the context of the application, an attacker gaining elevated privileges, blocking access to a Bluetooth device, or bypassing security restrictions.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate updates provided by Google Android or mobile carriers to vulnerable systems, immediately after appropriate testing.
- Remind users to download apps only from trusted vendors in the Play Store.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

REFERENCES:

Google:

http://source.android.com/security/bulletin/2016-03-01.html

CVE:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0815
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0816
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1621
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0818
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0728
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0821
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0823
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0824
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0826
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0827
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0828
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0829
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0830
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0831
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0832